(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
20 janvier 2005 (20.01.2005)

PCT

(10) Numéro de publication internationale
WO 2005/006645 A1

(51) Classification internationale des brevets[7] : H04L 9/30

(21) Numéro de la demande internationale :
PCT/FR2004/001743

(22) Date de dépôt international : 5 juillet 2004 (05.07.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
03/08229 4 juillet 2003 (04.07.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : THOMSON LICENCING S.A. [FR/FR]; 46 quai Alphonse Le Gallo, F-92100 BOULOGNE BILLANCOURT (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : ANDREAUX, Jean-Pierre [FR/FR]; 20 rue de Lorgeril, F-35000 RENNES (FR).

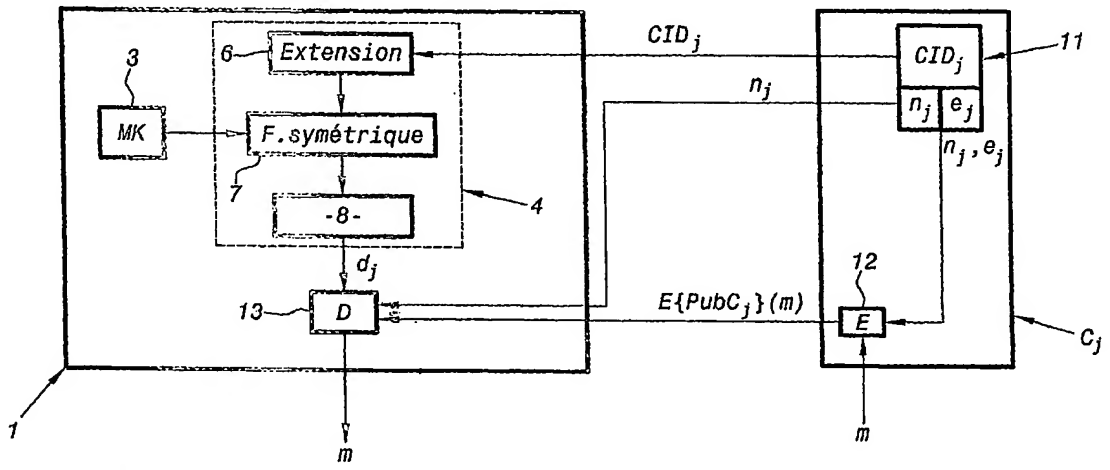
(74) Mandataires : HABASQUE, Etienne etc.; Cabinet LAVOIX, 2, Place d'Estienne d'Orves, F-75441 PARIS CEDEX 09 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH,

[Suite sur la page suivante]

(54) Title: METHOD FOR ENCODING/DECODING A MESSAGE AND ASSOCIATED DEVICE

(54) Titre : PROCEDE DE CHIFFREMENT/DECHIFFREMENT D'UN MESSAGE ET DISPOSITIF ASSOCIE



7... F. SYMMETRICAL

(57) Abstract: The invention relates to a method for encoding/decoding messages which are exchanged between a secure device (1) and a defined client device (Cj) in a network of client devices and to a secure device. The method comprises the following steps: asymmetrical cryptographic operations are performed by the secure device (1) and by the defined client device (Cj) respectively with the aid of a private key (nj, dj) and a public key (nj, ej); the private key (nj, dj) corresponding to the public key (nj, ej) of the defined client device (Cj) is determined on the basis of a secret master key (MK) stored in the secure device and at least one public data item (nj, CIDj) sent by the defined client device (Cj).

(57) Abrégé : L'invention concerne un procédé de chiffrement/déchiffrement de messages ô échanger entre un dispositif sécurisé (1) et un dispositif client défini (Cj) dans un réseau de dispositifs clients ainsi qu'un dispositif sécurisé. Le procédé comprend les étapes de : - réalisation d'opérations de cryptographie asymétrique par le dispositif sécurisé (1) et par

[Suite sur la page suivante]

WO 2005/006645 A1

PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **États désignés** *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

le dispositif client défini (Cj) respectivement ô l'aide d'une clé privée (nj, dj) et d'une clé publique (nj, ej), et - détermination de la clé privée (nj, dj) correspondant ô la clé publique (nj, ej) du dispositif client défini (Cj), ô partir d'une clé maîtresse secrète (MK) stockée dans le dispositif sécurisé, et d'au moins une donnée publique (nj, CIDj) envoyée par le dispositif client défini (Cj).